

La Revue
des Droits
de l'Homme

La Revue des droits de l'homme

Revue du Centre de recherches et d'études sur les
droits fondamentaux

Actualités Droits-Libertés | 2016

La CJUE encadre sévèrement les échanges de données entre administrations

Protection des données personnelles (CDFUE et Directive 2005/46/CE)

Jean-Philippe Foegle



Édition électronique

URL : <http://journals.openedition.org/revdh/1803>

DOI : 10.4000/revdh.1803

ISSN : 2264-119X

Éditeur

Centre de recherches et d'études sur les droits fondamentaux

Référence électronique

Jean-Philippe Foegle, « La CJUE encadre sévèrement les échanges de données entre administrations », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 12 février 2016, consulté le 19 avril 2019. URL : <http://journals.openedition.org/revdh/1803> ; DOI : 10.4000/revdh.1803

Ce document a été généré automatiquement le 19 avril 2019.

Tous droits réservés

La CJUE encadre sévèrement les échanges de données entre administrations

Protection des données personnelles (CDFUE et Directive 2005/46/CE)

Jean-Philippe Foegle

- 1 « N'oublions pas, enfin, qu'une des pierres angulaires des « hotspots » est l'identification et le fichage des candidats à l'installation en Europe. On peut même se demander si, finalement, le véritable objet de tout ce dispositif de relocalisation n'est pas de fichier et de tracer, dès leur arrivée, les étrangers qui entrent en Europe »¹. D'Athènes à Paris, les politiques d'immigration apparaissent toutes entières tournées vers un même objectif : celui la déterritorialisation des contrôles des Etats par la mise en place d'une catégorisation et d'un suivi toujours plus pointilleux des étrangers. Conséquence immédiate de ces évolutions : le recueil des données personnes des étrangers se trouve placé au cœur des nouvelles politiques de sécurité, l'objectif étant de permettre les connexions et les échanges de données² pour catégoriser, suivre des étrangers et détecter « le véritable motif de voyage des individus dans un contexte de mobilité de plus en plus intense »³. C'est ainsi que la multiplication des dispositifs de contrôle sur le vivant participent d'un glissement décrit par Foucault il y a plus de 30 années⁴ : le glissement d'un « Etat de territorialité » vers un « Etat de population », où le contrôle des Etats ne s'exerce plus tant sur des espaces territoriaux que sur des populations - sur le « vivant » - via des technologies biopolitiques
- 2 L'article 25 du projet de loi « immigration et nationalité », en cours d'adoption au Parlement, participe de cette logique, et est à envisager à ce titre de conjointement avec l'article 8 de ce même projet, qui permet aux préfetures de convoquer les étrangers titulaires d'un titre de séjour pluriannuel à des entretiens, afin de vérifier des éléments de leur situation et procéder le cas échéant au retrait de leur titre de séjour. Cette disposition, fortement contestée tant par les associations et les travailleurs sociaux que par la Commission Nationale des Droits de l'Homme⁵ qui y a vu « une atteinte

disproportionnée aux libertés individuelles et au secret professionnel, notamment des travailleurs sociaux », permettra désormais aux préfetures de requérir auprès d'autorités privées et publiques tous » documents et [les] informations nécessaires » (sic) au contrôle de la sincérité des déclarations et pièces fournies à l'appui d'une demande de titre de séjour. Une telle rédaction, qui ne précise pas la nature des données qui pourront être collectées ni les modalités exactes de collecte de celles-ci, offre aux préfetures le pouvoir de collecter une masse importante et indistincte de données de tous types. Et ce, d'autant plus que la liste des responsables de traitement de données après lesquels ces données⁶ pourront être collectées a été définie de manière plus qu'extensive, incluant nombre d'administrations et d'organismes chargés d'une mission de service public, mais également des personnes privées telles que les « établissements bancaires », les « fournisseurs d'énergie, de télécommunication et d'accès internet » et les « établissements de soins publics et privés ». Enfin et ce n'est pas l'aspect le moins préoccupant de cette disposition, ces données pourront être collectées « sans qu'y fasse obstacle le secret professionnel autre que le secret médical ». En clair et nous y reviendrons plus longuement (cf. infra 3°) ce nouvel article constitue un pas supplémentaire, inédit, dans la déconstruction de la vie privée des étrangers.

- 3 Cette présentation du développement presque inexorable des dispositifs de surveillance ne serait toutefois pas honnête si elle faisait l'impasse sur les nombreux « contre-feux » s'opposant à ceux-ci. Paradoxalement, c'est de l'Union européenne que viennent les ressources argumentatives les plus pertinentes pour limiter l'impact de ces politiques, et plus particulièrement de la jurisprudence de la Cour de justice de l'Union en matière de protection des données personnelles. Initialement envisagée à titre principal comme une modalité de construction du marché commun, limitée au « premier pilier » de l'Union et liée à des justifications de nature économique⁷ la protection des données personnelles dans l'Espace de Liberté, de Sécurité et de Justice est désormais fondé de manière croissante une rhétorique fondée sur les droits de l'homme. Comme en témoigne le récent arrêt « Schrems⁸ mais également l'arrêt « Digital Rights Ireland »⁹, l'opposition au développement de la surveillance apparaît, semble-t-il, comme l'occasion rêvée pour la Cour de légitimer son rôle de gardien du supposé ordre constitutionnel européen en opposant au modèle Nord-Américain de protection des données personnelles une conception « humaniste » de la vie privée, que d'aucuns nomment désormais l'« autodétermination informationnelle »¹⁰. En résulte une démarche constructive tendant à sauvegarder les droits procéduraux des citoyens européens pour garantir leur droit à contrôler les usages de leurs données ou, à minima, d'en connaître l'usage. Ce droit à l'« autodétermination », fondé en large partie sur l'illusion de l'autonomie du sujet de droit nanti de ses droits à l'information et sur une forme de fétichisme de la transparence, n'est pas, soulignons-le, exempt d'ambiguïtés¹¹. Il offre néanmoins nombre d'arguments mobilisables à l'appui de la défense des personnes dont les données seraient traitées de manière non transparentes. Ce n'est sans doute pas un hasard, dès lors, que la question des échanges de données entre administrations ait été traitée par un arrêt « Bara » du 1er octobre 2015, passé relativement inaperçu, mais qui paraît de nature à forcer le gouvernement à revoir sa copie ou, à tout le moins, lui donner du fil à retordre.
- 4 Loin des considérations abstraites sus-énoncées, le litige en cause concernait plus prosaïquement des assujettis roumains au régime d'assurance maladie, qui s'étaient vu contraints au paiement d'arriérés de contributions sociales. Le montant de ces arriérés avait été calculé par les organismes sociaux sur la foi de données relatives à leurs revenus

déclarés transmises par l'administration fiscale. Peu enclins à procéder au paiement exigé, les requérants avaient saisi la cour d'appel de Cluj d'un recours contestant la légalité du transfert des données fiscales relatives à leurs revenus au regard de la directive 95/46 sur la protection des données personnelles. Ceux-ci faisaient notamment valoir que leurs données avaient été transmises et utilisées sur la base d'un simple protocole interne et non d'une loi, et que celles-ci avaient été transmises et utilisées à des fins autres que celles pour lesquelles elles avaient été initialement communiquées à l'administration fiscale, le tout sans leur consentement et sans leur information préalable. En réponse, le gouvernement roumain avait insisté sur le fait que la transmission et le traitement des données personnelles en cause constituaient le corollaire des obligations de collaboration pesant sur les institutions publiques en vertu du code de procédure fiscal Roumain, le protocole se bornant à réglementer les modalités de transmission des données de l'Administration fiscale vers les organismes sociaux. De plus, ces obligations de transmission d'informations fiscales, qui ont pour but de définir le montant de l'impôt et des contributions dues à l'assurance maladie poursuivraient donc un objectif légitime de protection des intérêts financiers relevant des dispositions de l'article 13, paragraphe 1, sous e), de la directive 95/46/CE sur la protection des données personnelles.¹² Par conséquent, l'information des personnes concernées ne serait pas requise.

- 5 Saisi d'un doute sur la portée des articles 10 et 11 de la directive de 1995 instaurant une obligation d'information des personnes sur le transfert et le traitement subséquent de leurs données, les juges roumains ont sursis à statuer et renvoyé à la CJUE une question préjudicielle.
- 6 La question de droit portait alors principalement sur les articles 10, 11 et 13 de la directive de 1995, qui instituent une obligation pour les responsables de traitements de données personnelles d'informer les sujets de droit du transfert de leurs données personnelles vers d'autres administrations et du traitement subséquent de celles-ci, et ce en amont et en aval dudit transfert. En amont, l'article 10, qui concerne la collecte directe de données personnelles, exige que les personnes auprès desquelles le responsable du traitement des données a collecté ces dernières doivent pouvoir connaître l'existence des traitements et bénéficier d'informations concernant cette collecte¹³, et notamment les informations relatives aux finalités du traitement auquel les données sont destinées ainsi qu'aux destinataires ou aux catégories de destinataires de celles-ci. En clair, cet article exige a minima que les personnes soient informées de l'existence d'un transfert de leurs données vers une autre administration, et de la nature des données transmises. Un transfert vers une autre administration peut en effet constituer un changement dans les finalités poursuivies par le traitement de données¹⁴, ce qui est en principe prohibé si ces finalités sont incompatibles avec les finalités du traitement de données initial¹⁵. En aval, l'article 11, paragraphe 1, de la directive 95/46 envisage l'hypothèse des traitements de données collectées non pas auprès des personnes concernées, mais auprès d'autres responsables de traitement - en l'occurrence, une autre administration. Dans ces cas, les personnes concernées doivent bénéficier, dès l'enregistrement des données ou au plus tard lors de la première communication de celles-ci, d'une série d'informations, et notamment celles relatives aux finalités du traitement, aux catégories de données concernées et aux destinataires ou aux catégories de destinataires des données¹⁶.
- 7 Bien entendu, ces deux articles de la directive comportent de nombreuses dérogations. D'une part, l'article 13 de la directive énonce que les obligations d'informations prévues

aux articles 10 et 11 peuvent être limitées dès lors qu'une telle limitation constitue une mesure « nécessaire » pour sauvegarder un certain nombre d'intérêts légitimes, tels que la sûreté de l'État, la défense, la sécurité publique, la prévention et la répression des infractions pénales ou encore un intérêt économique ou financier important. D'autre part, l'article 11§2 prévoit que le responsable d'un traitement de données recueillies de manière indirecte peut s'abstenir d'informer la personne du transfert de ses données lorsque la législation prévoit expressément l'enregistrement ou la communication de ces dernières, et à condition que la mesure législative en cause ait institué des « garanties appropriées ». Dans ce cas précis, il n'est alors plus nécessaire de remplir les conditions énoncées à l'article 13 (poursuite d'un intérêt légitime) : il s'agit d'une exception au droit à l'information qui s'ajoute aux exceptions générales prévues à l'article 13. Il appartenait principalement à la Cour, ici, de déterminer dans quelle mesure la loi Roumaine -qui se contentait de prévoir la possibilité des transferts sans préciser leurs modalités et les garanties accordées aux personnes- pouvait être considérée comme remplissant les conditions des exceptions prévues par les articles 11§2 et 13 de la directive.

- 8 N'ayant pas été convaincue de la pertinence de l'argumentation du gouvernement Roumain la Cour juge invalide la législation roumaine permettant à une administration publique d'un État membre de transmettre des données personnelles à une autre administration publique et leur traitement subséquent, sans que les personnes concernées n'aient été informées de cette transmission ou de ce traitement. Le raisonnement de la Cour lie ici de manière étroite l'information des personnes concernées à leur droit de solliciter l'effacement de leurs données, prévu aux articles 12 et 14 de la directive de 1995 et protégé par la Charte des Droits Fondamentaux¹⁷. Surtout, cette information est liée à l'exigence de loyauté des traitements de données, qui conditionne la légalité de tout traitement de données personnelles et trouve également un fondement dans le droit primaire.
- 9 Ce faisant, la Cour consacre une évolution sans révolution. En effet, si les droits d'information des personnes avait déjà été consacrés comme corollaire du droit d'obtenir l'effacement des données dans les arrêts Rikeboer¹⁸ et Y.S et autres¹⁹, ce raisonnement n'avait jamais été étendu aux transferts de données entre administrations, pas plus qu'il n'avait à notre connaissance été directement fondé sur l'obligation générale de traitement loyal des données. Or, le droit à l'effacement des données et l'obligation de traitement loyal de celles-ci ayant désormais leur fondement dans le droit primaire de l'Union, il est désormais possible de considérer que l'information des personnes concernées constitue un véritable « droit », entouré à ce titre des mêmes garanties que les droits dont il conditionne l'exercice effectif (1°).
- 10 Ainsi formulé, ce « droit » doit nécessairement être entouré de garanties aussi strictes que les garanties entourant désormais le droit à l'effacement et l'obligation de traitement loyal des données, et ne peut en conséquence souffrir de limitations que dans des cas exceptionnels, par le biais de mesures nécessaires et proportionnées. En effet, l'information des personnes conditionnant l'exercice des droits consacrés sur le fondement des articles 8 et 7 de la Charte, toute restriction de l'un affecterait la portée de l'autre. (2°)
- 11 Sur le plan du droit interne Français, la portée de cet arrêt semble remettre au moins partiellement en cause la conventionalité de l'article 25 du projet de loi « immigration », qui apparaît loin de correspondre au niveau d'exigences implicitement fixé par la Cour.

1°/- Un double renforcement du « droit à l'information » des personnes sur le transfert de leurs données personnelles

- 12 Sans même que la Charte des Droits Fondamentaux ne soit mobilisée explicitement dans l'affaire Bara, celle-ci conduit nécessairement au renforcement de l'obligation d'information des personnes au prix d'un double effort de translation. En premier lieu, l'inclusion explicite du droit d'information des personnes dans une exigence de loyauté des traitements qui constitue une déclinaison de l'article 8 de la Charte des Droits Fondamentaux implique nécessairement que toute restriction de ce droit porte atteinte au contenu même du droit à la protection des données personnelles. **(A)** En second lieu, puisque le droit d'information constitue le corollaire nécessaire du droit à l'effacement des données non pertinentes qui trouve également un fondement dans la Charte des Droits Fondamentaux, une restriction du premier doit être vue comme une restriction du second et, partant, comme une restriction du contenu même du droit à la protection des données personnelles. **(B)**

A - L'information des personnes garantie par l'exigence de « loyauté » des traitements de données

- 13 Dans l'affaire en cause, il appartenait à la Cour de déterminer en premier lieu dans quelle mesure le recueil d'informations contenant les noms et les revenus des personnes constitue ou non un traitement de « données personnelles » au sens de cette même directive. La réponse faisait ici peu de doutes, la Cour ayant de longue date énoncé que constituent des données personnelles au sens de l'article 2a) de la directive, tant le « nom et le prénom de certaines personnes physiques dont le revenu excède certains seuils »²⁰ que « les revenus alloués par certaines entités [et] les bénéficiaires de ceux-ci »²¹. Par conséquent, la Cour énonce sans surprise que les données fiscales transférées à la CNAS par l'ANAF constituent des données à caractère personnel (Arrêt commenté, §29). Il est en revanche plus intéressant de constater que la Cour fonde, lato sensu, le droit d'information des personnes dont les données sont transférées d'une administration publique à l'autre sur « l'exigence de traitement loyal des données personnelles prévue à l'article 6 de la directive 95/46 » (Arrêt commenté, §33). Or, comme le rappelait l'avocat général dans ses conclusions²², la Cour avait d'ores et déjà jugé que les articles 6 et 7 -qui incluent le principe de loyauté, énoncé à l'article 6,1 a))- établissaient une liste exhaustive et limitative des conditions à remplir pour qu'un traitement de données à caractère personnel puisse être considéré comme licite. A contrario, tout traitement déloyal doit être considéré comme illicite²³.
- 14 L'insistance de la Cour sur les principes fondamentaux de licéité des traitements (articles 6 et 7) est d'autant moins anodine que la question préjudicielle ne portait nullement sur ces articles. Il s'agit donc très clairement d'un détournement visant à renforcer la juridicité de l'obligation d'information des personnes sur les finalités et modalités des traitements de données en rappelant que celle-ci découle de l'exigence plus générale de loyauté des traitements, qui touche au contenu même du droit à la protection des données personnelles. C'est à ce prix que la Cour peut d'autant plus se montrer exigeante à l'égard

des restrictions au droit à l'information des personnes : dès lors que la loyauté des traitements constitue une condition sine qua non de leur licéité et que l'information des personnes fait partie intégrante de l'exigence plus large de loyauté des traitements, toute restriction induite du droit à l'information entraîne nécessairement illicéité du traitement en cause.

- 15 Plus largement, rappelons que la dynamique interprétative à laquelle s'est livrée la Cour depuis quelques années a conduit à « relire » la directive de 1995 au regard des articles 8 et 7 de la Charte -garantissant respectivement le droit à la protection de données personnelles et le droit à la vie privée- et des objectifs généraux poursuivis par la Directive de 1995. Il découle en effet d'une jurisprudence constante de la Cour qu'il y a lieu, pour l'interprétation des dispositions du droit de l'Union, de tenir compte non seulement des termes de celles-ci, mais également de leur contexte et des objectifs poursuivis par la réglementation dont elles font partie²⁴, à savoir le fait de garantir une protection élevée et effective des personnes contre les traitements de données abusifs²⁵. Nombre de ses dispositions ont ce faisant été élevées au rang de garanties nécessaires au respect de l'article 8 de la Charte des Droits Fondamentaux garantissant un droit autonome à la protection des données personnelles, qu'elles viennent rendre effectif et préciser²⁶. Implicitement mais nécessairement, c'est ici l'obligation d'information qui se trouve élevée au rang de garantie nécessaire au respect du droit à la protection des données personnelles.
- 16 Le renforcement de la portée des dispositions de la Directive n'est d'ailleurs nullement étonnant si l'on considère que la directive de 1995 est antérieure à la rédaction et l'entrée en vigueur de la Charte des Droits Fondamentaux de l'Union Européenne et que l'article 8 de cette dernière se réfère explicitement -dans les explications sur la charte²⁷- et directement à la directive 2005/46/CE, ainsi qu'à la convention no 108 du Conseil de l'Europe du 28 janvier 1981 et à la jurisprudence issue de l'article 8 de la convention européenne de sauvegarde des droits de l'homme²⁸.
- 17 Plus largement, l'exigence de loyauté des traitements de données figure explicitement dans l'article 8 de la Charte²⁹ et met concrètement en œuvre, comme le rappelait l'avocat général Kokott, une exigence plus large de transparence et de prévisibilité des traitements de données personnelles³⁰. Or, cette exigence de prévisibilité est commune au droit de l'Union Européenne et au Droit de la Convention Européenne des sauvegarde des droits de l'Homme les juges ayant à de nombreuses reprises rappelé aux Etats-membres la nécessité de rédiger les lois « avec assez de précision pour permettre à toute personne, en s'entourant au besoin de conseils éclairés, de régler sa conduite »³¹. La jurisprudence de la Cour depuis 2005³² tend largement à appliquer ce qui s'apparente à un test d'« attente légitime » ou d'« aspiration raisonnable » à la vie privée. Dans ce cadre -et l'avocat général le soulignait dans ses conclusions³³- l'un des éléments les plus importants de l'exigence de « prévisibilité » des traitements de données tient à la spécification de finalités déterminées et légitimes, énoncée dans l'article 6 de la directive³⁴ et dans l'article 8 de la Charte. Bien que ses avis ne soient pas contraignants, le G29 a instauré une grille de lecture fort utile en la matière. Il s'agit en premier lieu, d'une part, d'examiner la relation entre les finalités poursuivies par la collecte initiale et les finalités poursuivies par l'usage ultérieur des données, qui ne doivent pas a priori présenter un lien trop ténu et devraient contribuer aux mêmes buts³⁵. D'autre part, il s'agit également d'examiner le contexte dans lequel la collecte de données est effectuée, et notamment le fait que la personne dont les données ont été collectées puisse ou non raisonnablement s'attendre à

ce que ses données soient réutilisées par la suite. Dans ce cadre, comme le souligne le groupe de travail « Article 29 »³⁶, plus la collecte est ciblée est spécifique, plus le titulaire des données doit pouvoir raisonnablement s'attendre à ce que ses données ne soient pas réutilisées.³⁷

- 18 En clair et pour revenir au sujet qui nous préoccupe -l'obligation d'information des personnes-, un traitement de données ne peut être considéré comme « loyal », et donc licite, qu'à la condition que les sujets de droit puissent être capables de déterminer avec suffisamment de précision le sort ultérieur de leurs données, afin de pouvoir le cas échéant refuser de consentir à la collecte de leurs données personnelles ou, à minima, faire invalider tout traitement incompatible avec les finalités pour lesquelles ces données ont été initialement collectées. Or, dès lors que l'information des personnes est considérée comme faisant partie intégrante de l'exigence plus générique de loyauté des traitements de données et que cette obligation conditionne le respect du droit à la protection des données personnelles, toute restriction du champ de cette obligation porte nécessairement atteinte au droit à la protection de données personnelles reconnu par l'article 8 de la Charte. Le changement est subtil mais néanmoins spectaculaire : dès lors que le droit à l'information est pleinement inclus dans l'exigence de loyauté des traitements, toute restriction générale de celui-ci dans le cadre de la mise en place d'un traitement de données instaure une présomption lourde d'illicéité dudit traitement.

B - L'information des personnes garantie par le « droit à » l'effacement des données non pertinentes

- 19 Surtout, la Cour rappelle également, dans la lignée des conclusions de l'avocat général³⁸ et d'un précédent arrêt Rijkeboer³⁹, que cette exigence d'information des personnes constitue une « condition nécessaire » à l'exercice par ces personnes de leur droit d'accès et de rectification des données traitées, défini à l'article 12 de la directive 95/46, et de leur droit d'opposition au traitement desdites données, visé à l'article 14 de cette directive (Arrêt commenté, §33) . Or, la possibilité d'obtenir l'effacement et la rectification des données personnelles indûment traitées figure explicitement dans le libellé de l'article 8 de la Charte des Droits Fondamentaux et constitue désormais une exigence conditionnant le respect du contenu même du droit fondamental à la vie privée.
- 20 En effet, la Cour a souligné itérativement la nécessité de se fonder sur une interprétation de la directive 95/46/CE permettant d'assurer un juste équilibre entre les différents droits et libertés fondamentales protégés par l'ordre juridique de l'Union⁴⁰ dans lequel le droit à la vie privée garanti par la Convention européenne des droits de l'homme revêt une signification particulière⁴¹. Or, cette recherche d'une interprétation de la directive conforme aux droits fondamentaux a conduit le juge de Luxembourg à fonder le droit à l'effacement sur les articles 7 et 8 de la Charte des droits fondamentaux. Dans l'arrêt Google Spain, la Cour a en effet qu'une personne peut demander l'effacement de données publiques devenues non pertinentes non pas uniquement au regard des articles 12 et 14 de la directive de 1995, mais plus largement et « eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte »⁴², ce qui signifie que les mécanismes institués par les articles 12 et 14 de la directive ont désormais un ancrage direct dans la Charte des Droits Fondamentaux de l'Union.
- 21 De manière plus significative encore, dans le récent arrêt Schrems⁴³, la Cour a invalidé le régime de transfert des données personnelles vers les Etats-Unis en rappelant que les

articles 7 et 8 de la Charte des Droits Fondamentaux exigent que les personnes « disposent de garanties suffisantes permettant de protéger efficacement leurs données contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données ». Or, le droit américain ne remplissait pas cette condition, entre autres, en raison de l'absence de « voies de droit administratives ou judiciaires permettant, notamment, d'accéder aux données les concernant et, le cas échéant, d'obtenir leur rectification ou leur suppression »⁴⁴. Le considérant 95 de la décision fonde au surplus ce droit à l'effacement -qui est autonome du droit prévu aux article 12 et 14 de la directive- sur le droit fondamental au recours, l'absence en droit Américain de droit « d'exercer des voies de droit afin [...] d'obtenir la rectification ou la suppression de telles donnée » ne respectant pas « le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte. », car « l'existence même d'un contrôle juridictionnel effectif destiné à assurer le respect des dispositions du droit de l'Union est inhérente à l'existence d'un État de droit ». Une analyse similaire pourrait être réalisée sous l'angle 13 de la Convention Européenne des Droits de l'Homme, puisque les juges de Strasbourg avaient conclu – dans l'arrêt Rotaru et dans une série d'arrêts ultérieurs- à l'inconventionnalité, sous l'angle de l'article 13 de la Convention, d'une disposition du droit roumain ne permettant aux requérants de contester la détention par les services de renseignements de données sur leur vie privée ou de réfuter la véracité de ces informations.⁴⁵

- 22 Or, conformément à une jurisprudence constante, la protection du droit fondamental à la vie privée exige que les dérogations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du strict nécessaire⁴⁶. Il est ainsi clair, désormais, que l'obligation d'information ne constitue pas une clause de style aisément dérogeable par le biais de l'article 13, mais qu'il s'agit bien d'une exigence forte du droit à la protection des données personnelles. En résulte sans nul doute une élévation significative des exigences de nécessité et de proportionnalité des atteintes à ce droit, puisque, s'agissant du droit à la vie privée et du droit à la protection des données personnelles, les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire », de sorte qu'il est nécessaire que s'exerce sur les limitations un « contrôle strict »⁴⁷
- 23 Restait à ce stade à examiner le contenu exact de cette obligation d'information, qui diffère selon que les données soient collectées directement auprès des personnes, ou de manière indirecte. S'agissant, de la collecte directe des données, l'article 10 de la directive prévoit que le responsable du traitement doit fournir à la personne l'identité du responsable du traitement de ces données, les finalités de ce traitement ainsi que « toute information supplémentaire nécessaire pour assurer un traitement loyal des données » dont « les destinataires ou les catégories de destinataires des données » ainsi que « l'existence d'un droit d'accès aux données [...] concernant [ladite personne] et de rectification de ces données ». La Cour conclut par suite que l'article 10 impose en principe aux responsables des traitements de données d'informer individuellement les personnes concernées de la transmission de ces données à une autre administration publique en vue de leur traitement par cette dernière. ((Arrêt commenté, §29). Le même raisonnement est suivi par les juges de Luxembourg s'agissant de l'accès indirect aux données prévu par l'article 11§1 de la Directive, ceux-ci jugeant que les autorités devaient à minima fournir aux requérants les informations prévues par les b) et c), de la directive 95/46, à savoir « l'identité du responsable du traitement, les finalités du

traitement « , mais également « les catégories de données concernées » ainsi que « l'existence d'un droit d'accès aux données la concernant et de rectification de ces données » (Arrêt commenté, §42).

- 24 En tout état de cause et sous réserve que les Etats-membres n'aient pas mis en œuvre les dérogations prévues aux articles 13 et 11§2 de la directive de 1995 le traitement loyal de ces données implique nécessairement que les personnes soient individuellement informées du transfert de leurs données ou, à minima, qu'elles soient informées explicitement et individuellement, en amont, que leurs données pourront faire l'objet d'un transfert vers d'autres responsables poursuivant d'autres finalités. Dans ce cas, il faudrait évidemment préciser la nature des destinataires éventuels des données et les finalités pour lesquelles celles-ci seraient alors traitées, mais également les cas dans lesquelles ces données peuvent faire l'objet d'un transfert.

*

2°/- Une restriction radicale des exceptions à l'obligation d'information sur les transferts de données personnelles

- 25 L'information des personnes concernées sur le transfert de leurs données apparaît ainsi fondée sur une double garantie issue du droit primaire de l'Union, celle de la prévisibilité de la législation d'une part, et du droit d'obtenir l'effacement de leurs données d'autre part. Les garanties entourant le droit à l'information des personnes et les garanties entourant le droit à la protection des données personnelles sont étroitement corrélées, et doivent être lues « en miroir ». Pour cette raison, les dérogations possibles au droit à l'information doivent être l'Union doivent répondre aux mêmes critères de nécessité que les dérogations admises à la protection des données à caractère personnel (A). Dans ce cadre, n'est-il pas à craindre que la première victime - innocente (?) - de l'arrêt Bara soit l'article 25 du projet de loi « immigration » ? (B)

A - Des restrictions cantonnées au strict nécessaire

- 26 La Cour a le loisir de rappeler à maintes occasions que le caractère « nécessaire » des mesures prises sur le fondement de l'article 13 conditionne la faculté accordée aux États membres de déroger à l'obligation d'information des personnes⁴⁸. L'arrêt Bara renforce et élargit ce critère de « nécessité ». A partir de cette grille de lecture et après avoir brièvement examiné les raisons ayant poussé la Cour à invalider la législation Roumaine, il conviendra alors d'examiner les caractères que devraient revêtir une loi limitant le droit d'information des personnes dont les données font l'objet d'un transfert, tant sur la forme que sur le fond.
- 27 Mais revenons au raisonnement de la Cour. Lui restait à ce stade à examiner dans quelle mesure le droit Roumain pouvait être considéré comme entrant dans l'une des exceptions à l'obligation d'information des personnes dont les données sont traitées, et qui sont énoncées respectivement aux articles 11§2 (collecte indirecte de données) et 13 de la directive (collecte directe de données). S'agissant de la collecte de données auprès des

personnes concernées, l'article 13 prévoit que les États membres peuvent s'abstenir d'informer les personnes lorsque cela s'avère nécessaire pour sauvegarder « un intérêt économique ou financier important d'un État membre [...] y compris dans les domaines monétaire, budgétaire et fiscal » ainsi qu'« une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e) », ce qui était le cas en l'espèce (Arrêt commenté, §39). Cependant, cette limitation doit être effectuée par le biais d'une mesure législative, qui doit présenter un degré suffisant de précision. Or, l'article 315 de la loi Roumaine n° 95/2006 n'avait fait qu'envisager, en son principe, la transmission de ces dernières données personnelles détenues par des autorités, des institutions publiques et d'autres institutions, et ce sans fixer avec une précision suffisante la liste des informations transmissibles ainsi que les modalités de mise en œuvre de cette transmission. Ces informations avaient été de plus élaborées au moyen non pas d'une mesure législative, mais d'un protocole de 2007 conclu entre deux administrations, lequel n'aurait pas fait l'objet d'une publication officielle et ne serait pas opposable. (Arrêt commenté, §40). De plus, les données relatives aux revenus ne font pas partie des données personnelles nécessaires à l'établissement de la qualité d'assuré en droit Roumain, de sorte que les personnes dont les données avaient été collectées ne pouvaient s'attendre légitimement à ce que celles-ci soient utilisées en vue de cette finalité (Arrêt commenté, §37). Faute de précisions suffisantes quant aux modalités et au contenu des restrictions qu'elle apportait au droit à l'information, la législation Roumaine est jugée non conforme au droit de l'Union. Un raisonnement du même type est suivi par la Cour s'agissant cette fois-ci de l'information devant être fournies aux personnes par le responsable d'un traitement de données qui n'ont pas été collectées auprès directement, mais auprès d'une autre institution. Ici, l'article 11§2 de la directive prévoit la possibilité de ne pas informer les personnes concernées lorsque la législation prévoit expressément l'enregistrement ou la communication des données, étant précisé que les États membres doivent dans ce dernier cas prévoir des « garanties appropriées » (Arrêt commenté, §46). Or, précisément, la loi Roumaine n'instaurait pas ce type de garanties en raison du caractère très vague et peu précis de la loi n'instaurait pas ce type de garanties.

- 28 Quelle devrait être, alors, le niveau de précision d'une loi, et l'ampleur des garanties instaurées par celle-ci ? Dans la mesure où l'information des personnes apparaît fondée sur une garantie fondée directement sur le droit à la protection des données personnelles, **toute limitation de ce droit ne pourrait être qu'étroite et se fonder sur des garanties suffisantes** puisque « les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire ». Il est alors pertinent de raisonner par analogie avec les arrêts les plus récents et les plus significatifs en la matière.
- 29 La Cour a mis en exergue, dans son arrêt *Digital Rights Ireland e.a.*, l'importance de prévoir des « règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte »⁴⁹. Une telle ingérence doit, selon la Cour, être « précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire »⁵⁰. Une telle exigence est d'autant plus forte que les restrictions admises à l'article 8 de la Charte des droits fondamentaux correspondent restrictions admises à l'article 8 de la Cour EDH, ce qui renforce au surplus l'exigence d'accessibilité et de précision. Or, une jurisprudence constante de la Cour dans le contexte de l'article 8 insiste sur la nécessité de rendre les modalités de collecte de

données accessibles et prévisibles. Ainsi, dans la Série des arrêts Rotaru⁵¹, S. et Marper⁵² et Kennedy⁵³, les juges de Strasbourg ont exigé que la loi soit à la fois accessible -étant entendu que les personnes ne devraient pas avoir à saisir les juridictions pour obtenir ces informations- et prévisible. L'accessibilité implique, aux yeux de la Cour, que les lois prévoyant des collectes de données soient dûment publiées.

- 30 La prévisibilité de la législation implique quant à elle que soient précisées les circonstances dans lesquelles les individus peuvent faire l'objet d'une collecte de leurs données, ainsi que les conditions dans lesquelles les autorités publiques peuvent mettre en œuvre cette collecte. Plus largement, la loi doit définir clairement et explicitement le type d'informations pouvant être consignées, les catégories de personnes pouvant être visées par cette collecte, les circonstances dans lesquelles cette collecte peut intervenir, les personnes qui ont le droit de consulter les informations enregistrées, et doit enfin fixer des limites précises à la conservation des données.⁵⁴
- 31 Or, puisque le droit à l'information touche directement au contenu du droit à la protection des données personnelles, les garanties entourant le droit doivent répondre aux mêmes exigences. Ainsi, une loi prise en application de l'article 13 de la directive devrait limiter la restriction de l'obligation d'information à ce qui est strictement nécessaire à la réalisation des objectifs poursuivis. La Commission rappelait d'ailleurs au cours de l'audience de l'affaire Bara que s'il peut être admis que le fonctionnement du service public d'assurance maladie constitue bien un objectif d'intérêt général au sens de l'article 13 de la directive 95/46 il serait en revanche difficile de comprendre en quoi il serait nécessaire d'omettre d'informer les personnes concernées puisque "cette information n'étant pas susceptible de porter atteinte à la réalisation dudit objectif"⁵⁵.
- 32 Surtout, celle-ci devrait préciser en détail les circonstances, les modalités et les conditions dans lesquelles les autorités nationales peuvent déroger à leur obligation d'information, conformément inter alia à la jurisprudence précitée de la CEDH. En toute hypothèse, une neutralisation de portée générale du droit à l'information des personnes est désormais inenvisageable.

B - L'article 25 du projet de loi « immigration » : future « victime » de l'arrêt Bara ?

- 33 Avant de s'intéresser au fond du problème – celui de la compatibilité de l'article 25 du projet de loi au regard de la directive 95/46/CE et du droit primaire de l'UE – il paraît pertinent de revenir de manière brève sur les évolutions de cette disposition au cours de la procédure d'adoption de la loi. Tel qu'il est actuellement rédigé, l'article instaure, en dérogation des articles 6 et 39 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, un droit de communication pour les préfetures qui emporte obligation, pour les autorités et personnes privées énumérées dans le nouveau texte, de transmettre à l'administration les données qu'elles détiennent relatives aux étrangers. Sont astreints à cette obligation : les administrations fiscales, les administrations chargées du travail et de l'emploi, les collectivités territoriales, les organismes de sécurité sociale, les autorités dépositaires des actes d'état civil, les chambres consulaires, les établissements scolaires et d'enseignement supérieur, les fournisseurs d'énergie, de télécommunication et d'accès à internet, les établissements de soins publics et privés, les établissements bancaires et organismes financiers, les entreprises de transport de

personnes et les greffes des tribunaux de commerce. Cet inventaire à la Prévert ouvre un très large pouvoir de collecte des données personnelles des étrangers.

- 34 Alors que la rédaction initiale de l'article rendait possible un exercice systématique de ce droit de communication, l'article 25 dans sa nouvelle rédaction prévoit explicitement que la communication des données intervient « sur demande de l'autorité administrative compétente, de manière ponctuelle et à titre gratuit » De même, l'article prévoit désormais que les étrangers peuvent demander la rectification, la mise à jour ou l'effacement de leurs données « si elles sont inexactes, incomplètes ou périmées, ou si leur collecte, leur utilisation, leur communication ou leur conservation n'est pas compatible avec les finalités déterminées au premier alinéa du présent article. » Surtout, est prévu un embryon de droit d'information de l'étranger, puisque l'autorité administrative est désormais tenue d'informer la personne dont elle s'apprête à retirer la carte de séjour sur le de la teneur et de l'origine des informations et documents ainsi obtenus sur le fondement du droit de communication, et se doit de communiquer « une copie des documents susmentionnés à l'intéressé s'il en fait la demande. ». Enfin, à la suite d'un amendement no 115, accepté le 26 janvier par la commission des lois de l'Assemblée Nationale et le Gouvernement, les données de connexion sont désormais exclues du champ d'application de l'article.
- 35 Malgré cette progression en demi-teinte des droits des étrangers, il paraît peu probable que cet article puisse résister à un éventuel contrôle de conventionalité, et ce pour nombre de raisons. Soulignons toutefois d'emblée qu'il est improbable que cette disposition puisse être remise en cause au regard des conditions de fond que doivent remplir les traitements de données, puisque la Cour a principalement condamné, dans ses arrêts *Digital Rights Ireland* et *Schrems*, des systèmes prévoyant une collecte systématique et non ciblée des données des personnes -ce qui signifie a contrario qu'une collecte ponctuelle, ciblée et dûment justifiée peut être légitime. Toutefois et bien que cela dépasse le champ de la présente lettre, l'on peut s'interroger sur la pertinence de permettre la collecte de certaines données-qui pourraient fort bien ne pas remplir le critère de « nécessité » maintes fois évoqué dans la présente lettre.
- 36 En premier lieu, le moment à partir duquel intervient l'information individuelle de l'étranger, à savoir le moment où l'autorité envisage le retrait du titre, ne correspond aucunement aux exigences du droit européen. En effet, la directive précise que cette information doit intervenir « dès l'enregistrement des données ». Or, le préfet ayant une obligation d'examen individuel des dossiers des étrangers impliquant à tout le moins un examen approfondi des pièces de ce dossier, l'on imagine mal comment l'intention de retirer le titre de séjour pourrait, en tout légalité, intervenir de manière concomitante à l'enregistrement des données.
- 37 Reste alors à savoir si la loi immigration peut correspondre aux exceptions prévues par l'article 13 de la directive ou, en application de l'article 11§2 de celle-ci, tenir lieu d'information des étrangers sur la possibilité que leurs données fassent l'objet d'un traitement. Rappelons en tout premier lieu que l'article 13 de la directive de 1995 prévoit en tout état de cause qu'une loi ne peut restreindre le droit d'information des personnes que si celle-ci est nécessaire à la poursuite un certain nombre d'intérêts légitimes des Etats, tels que, inter alia, la sûreté de l'État, la défense, la sécurité publique, la prévention et la répression des infractions pénales, un intérêt économique ou financier important ou encore une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique.

- 38 Or d'une part, il paraît peu probable que la disposition en cause puisse correspondre à l'une des exceptions listées par cet article. D'une part, rappelons que la Cour a jugé que la directive 95/46 aboutit à une harmonisation qui est, en principe, complète⁵⁶, de sorte que la marge de manœuvre des Etats membres est largement réduite quant au fait de décider ce qui correspond ou ne correspond pas, dans leur droit national, aux exceptions de l'article 13. Or, l'exception de sécurité publique ou d'ordre public fait traditionnellement l'objet d'une interprétation restrictive de la Cour ; celle-ci énonçant itérativement depuis 1977 que « le recours par une autorité nationale à la notion d'ordre public suppose (...), l'existence, en dehors de tout trouble pour l'ordre social que constitue toute infraction à la loi, d'une menace réelle et suffisamment grave, affectant un intérêt fondamental de la société »⁵⁷. Plus récemment, dans l'arrêt Tsakouridis⁵⁸, la cour a énoncé que les « raisons impérieuses de sécurité publique » permettant l'éloignement d'un étranger impliquent « que le comportement de la personne concernée représente une menace réelle et actuelle pour un intérêt fondamental de la société ou de l'Etat membre d'accueil, constatation qui implique, en général, chez l'individu concerné, l'existence d'une tendance à maintenir ce comportement à l'avenir »⁵⁹.
- 39 Par analogie, il paraît donc pour le moins peu probable que le simple contrôle de la sincérité des déclarations des étrangers puisse correspondre à l'exception de « sécurité publique ». En effet, si l'article 25 du projet de loi fait bien référence à « l'authenticité des documents » fournis par l'étranger, qui pourrait éventuellement constituer la recherche d'atteinte à la sécurité publique ou une infraction dans le cas où il y aurait falsification de documents d'identité, cet article ne s'y limite pas, et le contrôle de la « sincérité des déclarations souscrites » fait référence à des mesures de police des étrangers qui ne visent pas nécessairement à prévenir des atteintes à l'ordre public stricto-sensu. Tous les étrangers qui se voient retirer leur titre de séjour n'ont pas nécessairement, en effet, commis d'infractions, pas plus qu'ils ne représentent dans tous les cas une menace à l'ordre public. Les dérogations prévues à l'article 13 étant les seules dérogations possibles à l'obligation pesant sur le responsable de traitement collectant directement (article 10) des données, l'on en déduit que toutes les administrations et personnes privées ont désormais l'obligation d'informer les étrangers, dès la première collecte de leurs données, que celles-ci pourront faire l'objet d'un transfert auprès des préfetures.
- 40 Et, quand bien même il serait possible d'intégrer l'article 25 dans une exception liée à la prévention des infractions ou à la sécurité publique, il paraît peu probable que celui-ci remplisse le critère de précision et nécessité étudié supra (cf. 1°). En effet, si la Cour a considéré dans son arrêt IPI⁶⁰, que l'absence d'information des personnes faisant l'objet d'un traitement de données par des détectives privés correspondait à une telle nécessité - et l'on comprend aisément pourquoi puisque ce type de traitement de données s'opère nécessairement de manière secrète -, l'on peine à trouver ce type de nécessités en s'agissant de la communication des données des étrangers.

41

Peut-on également envisager, en aval, que les préfetures soient soumises à l'obligation d'informer les étrangers de l'enregistrement de leurs données obtenues auprès des administrations et personnes privées dont la liste figure dans l'article 25 ? Cela paraît plus incertain dans la mesure où l'article 11§2 prévoit que les responsables de traitement peuvent être dispensés de leur obligation d'information lorsque la législation prévoit expressément l'enregistrement ou la communication des données, et à condition que cette dernière ait institué des garanties appropriées. Il s'agit d'une exception

supplémentaire à l'information des personnes, qui n'a pas besoin d'être « nécessaire ». Dans ce cadre, l'on considère que la publication d'une loi tient lieu d'information des personnes.

- 42 Toutefois, une loi de ce type doit être entourée des « garanties nécessaires », ce qui fait une fois de plus référence à la précision et la transparence de la législation, qui doit préciser a minima les circonstances dans lesquelles les individus peuvent faire l'objet d'une collecte de leurs données, ainsi que les conditions dans lesquelles les autorités publiques peuvent mettre en œuvre cette collecte. A cet égard, soulignons toutefois que le fait que qu'un décret soit amené à « définir de manière différenciée, pour chaque administration, organisme, établissement ou entreprise concernée, la nature des informations et des documents susceptibles d'être communiqués à l'autorité administrative »⁶¹ pourrait offrir une base suffisante à l'absence d'information des personnes. En effet, la notion de « mesure législative » n'implique pas nécessairement qu'un décret ne puisse pas constituer une telle mesure : dans l'arrêt *Bara*, la Cour faisait principalement grief au protocole de ne pas avoir été publié et de ne pas être opposable, et le rapporteur public rappelait qu'une mesure législative se devait d'être générale, publiée et opposable⁶² – ce qui serait le cas, en droit interne, d'un décret d'application.
- 43 Dans la mesure toutefois où l'obtention des informations par les préfectures coïncide avec la prise d'une décision de retrait d'un titre de séjour, il n'est pas inenvisageable qu'une argumentation liant l'information des personnes au Principe Général du Droit de l'Union Européenne du droit d'être entendu, bien que ce dernier soit désormais réduit à portion congrue⁶³
- 44 L'invalidation de l'article en cause apparaît néanmoins d'autant plus certaine que le texte du projet de règlement sur les données personnelles adopté par le parlement en première lecture précise quels sont les éléments qui doivent impérativement figurer dans une loi restreignant les obligations des responsables de traitements de données -et notamment l'obligation d'information- et qui, en l'occurrence, ne figurent manifestement pas dans la rédaction actuelle de l'article 25. Parmi ces éléments, figurent désormais non seulement les finalités du traitement de données, mais également l'identité du responsable de traitement, les moyens mis en œuvre par le traitement, les garanties mises en place contre les transferts de données, accès aux données ou traitements de données illégaux et, enfin, les modalités d'exercice du droit d'information des personnes. L'article 21 (2) précise en outre que la loi ne doit pas aller au-delà de ce qui est nécessaire au vu des objectifs poursuivis par le traitement. Or, un compromis entre le Parlement et le Conseil de l'Union Européenne ayant été trouvé, il paraît plus que probable que le texte soit adopté en l'état.
- 45 Rappelons enfin également qu'un droit de communication des données des étrangers - certes moins étendu dans son champ- est déjà prévu par le fichier AGDREF, et que les considérations sus-énoncées pourraient fort bien remettre en cause le fonctionnement actuel de ce fichier. L'obligation d'information devrait ainsi trouver à s'appliquer aux nombreux transferts de données personnelles concernant les étrangers entre les différentes administrations publiques⁶⁴.

*

**

- 46 Bien qu'il soit moins retentissant que l'arrêt Schrems, l'arrêt « Bara » contribue, lui aussi, à renforcer la protection des données personnelles dans l'Espace de Sécurité, de Liberté et de Justice. Et, si ses considérants paraissent anodins de prime abord et ne mobilisent pas le texte de droit primaire dont la force argumentative est la plus forte -la Charte des Droits Fondamentaux- sa portée est néanmoins d'une grande importance au regard de l'architecture générale de la protection de la vie privée dans l'Union Européenne. C'est en effet à un effort créatif d'interprétation du texte que la Cour s'est attelée, en procédant à une véritable redéfinition **de la directive pour permettre d'entourer de solides garanties le droit à l'information des personnes dont les données font l'objet d'un traitement automatisé**. Ainsi, l'objectif de protection élevé des droits fondamentaux dont la CJUE se veut -à juste titre - la gardienne permet une fois de plus de passer outre une lecture techniciste de la directive pour assurer la pleine effectivité des droits fondamentaux.
- 47 Sur le plan national, il paraît probable que la décision ait un impact très important sur le fonctionnement de nombre de fichiers, et en particulier certains fichiers concernant les étrangers tel que le fichier AGDREF. L'émergence de ce droit procédural à l'information permettra-t-il de renverser la tendance à et ses effets corrosifs sur le droit à la vie privée des étrangers ? Cela paraît fort peu probable, dans la mesure où l'invocation de la lutte contre l'« immigration irrégulière » fonctionne toujours de manière efficace lorsqu'il s'agit de permettre des atteintes aux droits fondamentaux des étrangers. A cet égard, l'impact social du fichage ne réside peut-être pas tant dans le fonctionnement concret des fichiers que dans les représentations que celui-ci véhicule de l'étranger : celui d'une catégorie « dangereuse » dont les restrictions des droits seraient, de ce fait même, plus aisément justifiables..
- 48 Futiles et illusoirs « lignes Maginot » relayées par un imaginaire technicien lié à la croyance ferme d'une infaillibilité et d'une neutralité de la technique⁶⁵, force est de constater que les politiques de fichage participent de la construction de la figure de l'étranger comme un « indésirable »⁶⁶.

*

- 49 CJUE, Troisième chambre, 1er octobre 2015, *Smaranda Bara e.a. contre Președintele Casei Naționale de Asigurări de Sănătate et autres*, Aff C-201/14
- 50 **Projet de loi portant diverses dispositions relatives à la maîtrise de l'immigration (INTX1412529L), article 25 – Version à jour du 26 janvier 2016.**

*

Les Lettres « Actualités Droits-Libertés » (ADL) du CREDOF (pour s'y abonner) sont accessibles sur le site de la Revue des Droits de l'Homme (RevDH) – Contact

NOTES

1. Elsa Bourdier et Jean- Philippe Foegle, « Entretien avec Madame Claire Rodier, directrice du GISTI (Groupe d'Information et de Soutien des Immigré.e.s) et co-fondatrice du réseau euro-africain Migreurop », *La Revue des droits de l'homme*[En ligne], 8 | 2015, mis en ligne le 24 novembre 2015
2. Sylvia Preuss-Laussinotte, « L'Union européenne et les technologies de sécurité », *Cultures & Conflits* [En ligne], 64 | hiver 2006, mis en ligne le 06 mars 2007, consulté le 17 janvier 2016. URL : <http://conflits.revues.org/2142>
3. Ayse Ceyhan, « Les technologies européennes de contrôle de l'immigration. Vers une gestion électronique des « personnes à risque » », *Réseaux* 1/2010 (n° 159) , p. 131-150
4. Michel Foucault, *Sécurité, Territoire, Population. Cours au Collège de France, 1977-1978, Paris, Seuil/Gallimard, 2004, p. 112.*
5. CNCDH, Assemblée plénière, « Avis sur la réforme du droit des étrangers (adoption : unanimité) », 21 mai 2015, NOR : CDHX1512299V, JORF n° 0159 du 11 juillet 2015
6. « Ce droit de communication s'exerce sur demande de l'autorité administrative compétente, de manière ponctuelle et à titre gratuit, quel que soit le support utilisé pour la conservation des documents, auprès : 2° Des autorités dépositaires des actes d'état civil ; 3° Des administrations chargées du travail et de l'emploi ; 4° Des organismes de sécurité sociale et de l'institution mentionnée à l'article L. 5312-1 du code du travail ; « 7° Des établissements scolaires et des établissements d'enseignement supérieur ; 8° Des fournisseurs d'énergie et des services de communications électroniques ; 9° Des établissements de santé publics et privés ; « 10° Des établissements bancaires et des organismes financiers ; 12° Des greffes des tribunaux de commerce. »
7. V. Notamment: Yves Poulet, « Transborder Data Flows and Extraterritoriality: The European Position », *J. Int'l Com. L. & Tech.*, 2007, vol. 2, p. 141.
8. CJUE, Grande Chambre, 6 octobre 2015, *Schrems v. Data protection commissioner*, Aff. C-362/14, V. Steve Peers, « The party's over: EU data protection law after the Schrems Safe Harbour judgment, EU Law Analysis, 7 octobre 2015.
9. CJUE, Grande Chambre, 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, affaires jointes C-293/12 & C-594/12. V. Florence Benoit-Rohmer, « Protection des données personnelles ; Note sous Cour de justice de l'Union européenne, grande Chambre, 8 avril 2015, *Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources et autres et Kärnter Landesregierung Seitlinger et autres*, affaires jointes numéros C-293/12 et C-594/12 », *RTDE* 2015, p. 168 Denys Simon, « La révolution numérique du juge de l'Union : les premiers pas de la cybercitoyenneté », *Europe* n° 7, p. 4 ; Marie-Laure Basilien-Gainche, « Une prohibition européenne claire de la surveillance électronique de masse », in *Revue des droits de l'homme*, 14 mai 2014
10. La notion d'« autodétermination informationnelle », s'oppose à une conception patrimoniale des données personnelles et inscrit la protection de l'autonomie individuelle dans une approche par les droits de l'homme. Chaque sujet de droit aurait désormais un droit à « la maîtrise de la circulation « légitime » de son image informationnelle. ». V. Antoinette Rouvroy, « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ? », in Stéphanie Lacour (dir.), *La sécurité de l'individu numérisé. Réflexions prospectives et internationales*, Paris, L'Harmattan, 2009, p. 2.
11. Gloria González Fuster, « Fighting For Your Right to What Exactly? The Convolved Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection », *Birkbeck Law Review* Volume 2(2), p. 263.

12. Voir sur ce point : Conclusions de l'Avocat général M. Pedro Cruz Villalón, présentées le 9 juillet 2015, Affaire C-201/14, §37

13. « Les États membres prévoient que le responsable du traitement ou son représentant doit fournir à la personne auprès de laquelle il collecte des données la concernant au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée : a) l'identité du responsable du traitement et, le cas échéant, de son représentant ; b les finalités du traitement auquel les données sont destinées ; c) toute information supplémentaire telle que : les destinataires ou les catégories de destinataires des données, –le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse, l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,

14. G29, 2 avril 2013, Opinion 03/2013 on purpose limitation, WP 203.

15. Conclusions de l'avocat général M. Niilo Jääskinen, 17 novembre 2011, Bonnier Audio AB contre Perfect Communication Sweden AB (« ePhone »), Affaire C-461/10, §51

16. « 1. Lorsque les données n'ont pas été collectées auprès de la personne concernée, les États membres prévoient que le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée : a) l'identité du responsable du traitement et, le cas échéant, de son représentant ; b) les finalités du traitement ; c) toute information supplémentaire telle que : les catégories de données concernées, les destinataires ou les catégories de destinataires des données, l'existence d'un droit d'accès aux données la concernant et de rectification de ces données [...]

17. CJUE, Grande Chambre, 13 mai 2014, Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González, Aff. C-131/12 – Communiqué de presse et ADL du 16 juin 2014

18. CJUE, Troisième chambre, 7 mai 2009, College van burgemeester en wethouders van Rotterdam contre M. E. E. Rijkeboer, Aff. C-553/07. V. Douwe Korff, « The proposed General Data Protection Regulation : suggested amendments to the definition of personal data », EU Law Analysis, 15 octobre 2014

19. CJUE, Troisième chambre, 14 juillet 2014, Y. S et autres, Aff. C-141/12 . Steve Peers, « Data protection rights and administrative proceedings », EU Law Analysis, 17 juillet 2014.

20. CJCE, 20 mai 2003, Österreichischer Rundfunk e.a. , Aff. C-465/00 § 64

21. CJUE, 12 septembre 2007, « Satakunnan Markkinapörssi et Satamedia » ,Aff.C-73/07, §35

22. Voir sur ce point : Conclusions de l'Avocat général M. Pedro Cruz Villalón, présentées le 9 juillet 2015, Affaire C-201/14, §54

23. CJUE, 24 novembre 2011, ASNEF et FECEMD, Aff. C-468/10 et C-469/10 , § 38 et 40 ; V. Conclusions de l'avocat général M. Niilo Jääskinen, 17 novembre 2011, Bonnier Audio AB contre Perfect Communication Sweden AB (« ePhone »), Affaire C-461/10, § 54

24. CJUE, Grande chambre, 19 décembre 2013, Koushkaki, C-84/12, EU :C :2013 :862

25. CJUE, 7 mai 2009, Huber, Aff. C-524/06, Rec. p. I-9705, §43 ; CJUE, 24 novembre 2011, ASNEF et FECEMD, Aff. C-468/10 et C-469/10 , § 25

26. V. en ce sens, De Hert, Paul, and Serge Gutwirth. "Data protection in the case law of Strasbourg and Luxembourg : Constitutionalisation in action." (2009) : 3-44.

27. Explications sur la Charte des Droits Fondamentaux de l'Union Européenne. Document CONVENT 49 du 11 octobre 2000

28. Voir sur ce sujet la fiche thématique « protection des données personnelles » du service de presse de la CEDH

29. « 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. [...] »

30. "L'exigence de prévisibilité a trouvé une expression particulière dans le droit de la protection des données qui impose que tout traitement de données soit lié à des fins déterminées, comme l'exige expressément l'article 8, paragraphe 2, de la charte ". V. Conclusions de l'avocat général Mme Juliane Kokott, 18 juillet 2007, Promusicae contre Telefónica de España SAU, Affaire C-275/06, §53

31. Cour EDH, 14 mars 2002, Gaweda c. Pologne, Req. n° 26229/95

32. V. sur ce point: Tomas Gomez-Arostegui, « Defining private life under the European convention on human rights by referring to reasonable expectations », *California Western International Law Journal*, 2005, vol. 35, no 2.

33. Voir sur ce point : Conclusions de l'Avocat général M. Pedro Cruz Villalón, présentées le 9 juillet 2015, Affaire C-201/14, §63

34. Article 6 : 1. Les États membres prévoient que les données à caractère personnel doivent être : [...]b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées [...] »

35. Idem, p. 23

36. Il s'agit d'un organe consultatif indépendant sur la protection des données et la vie privée, institué au titre de l'article 29 de la directive sur la protection des données. Il se compose de représentants des autorités nationales de l'Union compétentes en matière de protection des données, du CEPD et de la Commission. Il émet des recommandations, des avis et des documents de travail

37. Idem, p. 24

38. Voir sur ce point : Conclusions de l'Avocat général M. Pedro Cruz Villalón, présentées le 9 juillet 2015, Affaire C-201/14, §37

39. CJUE, Troisième chambre, 7 mai 2009, College van burgemeester en wethouders van Rotterdam contre M. E. E. Rijkeboer, Aff. C-553/07. V. Douwe Korff, « The proposed General Data Protection Regulation : suggested amendments to the definition of personal data », *EU Law Analysis*, 15 octobre 201

40. CJUE, 29 janvier 2008, Promusicae, Aff. C-275/06, Rec. p. I-271, § 68

41. CJUE, 18 juin 1991, ERT, C-260/89, Rec. p. I-2925, § 41

42. CJUE, Grande Chambre, 13 mai 2014, Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González, Aff. C-131/12 – Communiqué de presse et ADL du 16 juin 2014

43. CJUE, Grande Chambre, 6 octobre 2015, Schrems v. Data protection commissioner, Aff. C-362/14, V. Steve Peers, « The party's over: EU data protection law after the Schrems Safe Harbour judgment, *EU Law Analysis*, 7 octobre 2015.

44. Idem, §95

45. Cour. EDH, Gr. Ch., 4 mai 2000, Rotaru c. Roumanie, Requête no 28341/95 .

46. CJUE, 12 septembre 2007, « Satakunnan Markkinapörssi et Satamedia », Aff.C-73/07, §56, CJUE, 24 novembre 2011, ASNEF et FECEDM, Aff. C-468/10 et C-469/1, §77 et 86

47. CJUE, Grande Chambre, 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., affaires jointes C-293/12 & C-594/12, §78 V. Florence Benoit-Rohmer, « Protection des données personnelles ; Note sous Cour de justice de l'Union européenne, grande Chambre, 8 avril 2015, Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources et autres et Kärnter Landesregierung Seitlinger et autres, affaires jointes numéros C-293/12 et C-594/12 », *RTDE* 2015, p. 168 Denys Simon, « La révolution numérique du juge de l'Union : les premiers pas de la cybercitoyenneté », *Europe* n° 7, p. 4 ; Marie-Laure Basilien-Gainche, « Une prohibition européenne claire de la surveillance électronique de masse », in *Revue des droits de l'homme*, 14 mai 2014
48. CJUE, Troisième chambre, 7 novembre 2013, IPI, Aff. C473-12, §32
49. CJUE, Grande Chambre, 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., affaires jointes C-293/12 & C-594/12.
50. Idem
51. Cour. EDH, Gr. Ch., 4 mai 2000, Rotaru c. Roumanie, Requête no 28341/95
52. Cour.EDH, Gr.Ch., 4 décembre 2008, S. et Marper c. Royaume Uni, Req. n° 30562/04 et 30566/04. V., sur cet arrêt : Sylvie Peyrou-Pistouley, « L'affaire Marper c/ Royaume-Uni : un arrêt fondateur pour la protection des données dans l'espace de liberté, sécurité, justice de l'Union européenne », *RFDA* 2009, p. 94 ; Rocco Bellanova et Paul De Hert, « Le cas S. et Marper et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen », *Cultures & Conflits* [En ligne], 76 | hiver 2009, mis en ligne le 03 mai 2011,
53. Cour EDH, 4e Sect. 18 mai 2010, Kennedy c. Royaume-Uni, Req. n° 26839/05 – ADL du 20 mai 2010
54. V., pour une illustration récente : Cour. EDH, Gr. Ch., 4 décembre 2015, Zakharov c. Russie, Req. n° 47143/06
55. Voir sur ce point : Conclusions de l'Avocat général M. Pedro Cruz Villalón, présentées le 9 juillet 2015, Affaire C-201/14, §47
56. CJUE, 7 mai 2009, Huber, Aff. C-524/06, Rec. p. I-9705, §43, 50-51
57. CJCE, 27 octobre 1977, Régina c. Pierre Bouchereau, *Aff.* 30-77
58. CJUE, 23 novembre 2010, Tsakouridis, aff. C-145/0, ;Actualités droits-libertés du 6 janvier 2011 par Myriam BENLOLO-CARABOT*
59. Idem, §34
60. CJUE, Troisième chambre, 7 novembre 2013, IPI, Aff. C473-12, §32
61. V.Erwann Binet, RAPPORT FAIT AU NOM DE LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE SUR LE PROJET DE LOI (n° 2183) *relatif au droit des étrangers en France*,
62. Voir sur ce point : Conclusions de l'Avocat général M. Pedro Cruz Villalón, présentées le 9 juillet 2015, Affaire C-201/14, §85
63. M-L. BASILIEN-GAINCHE et T. RACHO, « Droit d'être entendu : quand le souci d'efficacité de l'éloignement l'emporte sur l'application effective des droits fondamentaux », in *Revue des droits de l'homme*, 21 novembre 2014 ; M-L. BASILIEN-GAINCHE, « Removal orders and the right to be heard: the CJEU fails to understand the dysfunctional French asylum system », in *EU Law Analysis*, 12 décembre 2014. X. DOMINO, « Droit d'être entendu et OQTF : un exemple de dialogue entre les jurisprudences », *AJDA*, 2014, 1501 ;Denys SIMON, « L'application de la Charte par les juges administratifs », *Europe*, n° 2, février 2014, p. 2 ; S. SLAMA, « Question préjudicielle sur le droit d'être entendu par l'administration préalablement à l'édition d'une OQTF », in *Revue des droits de l'homme*, 20 mars 2013 ; H. STILLMUNKES, « L'article 41 de la Charte des droits fondamentaux de l'Union européenne, le droit d'être entendu et la police des étrangers », *RFDA*, 2013, 839 ; Naïké Lepoutre, « Le droit d'être entendu avant l'adoption d'une mesure d'éloignement,

un droit fondamental réduit à portion congrue », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 06 janvier 2015.

64. V. En ce sens : Dictionnaire Permanent Droit des Etrangers, « La CJUE remet le droit à l'information au centre des transferts de données entre administrations », 21 octobre 2015.

65. Philippe Bonditti, « Biométrie et maîtrise des flux : vers une « géo-technopolis du vivant-en-mobilité » ? », *Cultures & Conflits* [En ligne], 58 | été 2005, mis en ligne le 10 octobre 2005

66. Emmanuel Blanchard, « Les "indésirables". Passé et présent d'une catégorie d'action publique », *Figures de l'étranger. Quelles représentations pour quelles politiques ?*, 2013, p. 16-26.

RÉSUMÉS

Le 1er octobre 2015, la Cour de Justice de l'Union Européenne a invalidé le régime juridique Roumain de transfert de données entre les administrations publiques. Il s'agissait, en l'espèce, de données relatives aux revenus transmises aux organismes sociaux par l'administration fiscale. Ce transfert de données avait été fondé sur une loi pour le moins imprécise, et complétée par un protocole interne non publié et non opposable. Se fondant sur l'article 11 de la Directive 2005/46/CE sur la protection des données personnelles, la Cour renforce l'exigence d'information des administrés dont les données font l'objet d'un transfert en l'ancrant dans une exigence plus large de garantir le traitement « loyal » des données personnelles et d'accès effectif au droit à l'effacement, deux exigences qui trouvent leur source dans l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Ainsi formulé, le droit à l'information ne souffre plus que de peu de limitations, qui doivent être réduites au strict nécessaire. La discussion et l'adoption probable d'un article du projet de loi immigration – l'article 25 – offrant aux préfetures un très large droit de se faire communiquer les données personnelles des étrangers, et ce en vue de contrôler la réalité de leurs motifs de séjour, redonne à cette décision toute son actualité.

AUTEUR

JEAN-PHILIPPE FOEGLE

Doctorant en droit public (CREDOF - Université Paris Ouest Nanterre) et allocataire doctoral (Conseil régional d'Ile de France)